Journal of Pure and Applied Algebra 52 (1988) 91–102
North-Holland

AN ELEMENTARY PROOF OF THE AUTOMORPHISM THEOREM FOR THE POLYNOMIAL RING IN TWO VARIABLES

James H. McKAY

Department of Mathematical Sciences, Oakland University, Rochester, MI 48309, U.S.A.

Stuart Sui-Sheng WANG

Department of Mathematical Sciences, Oakland University, Rochester, MI 48309, U.S.A.
Department of Mathematics, Purdue University, West Lafayette, IN 47907, U.S.A.

Communicated by C.A. Weibel
Received 10 July 1986
Revised 21 November 1986

If $\mathbf{k}$ is a field, then the automorphism theorem for $\mathbf{k}[x, y]$ states that every $\mathbf{k}$-algebra automorphism of $\mathbf{k}[x, y]$ is a finite compositional product of automorphisms of the type: (i) $x \mapsto x$, $y \mapsto y + h(x)$ with $h(x) \in \mathbf{k}[x]$; or (ii) $x \mapsto a_{11}x + a_{12}y + a_{13}$, $y \mapsto a_{21}x + a_{22}y + a_{23}$ with $a_{11}a_{22} \neq a_{21}a_{12}$ and $a_{ij} \in \mathbf{k}$. The proof presented in this paper, in the case of $\mathbf{k}$ being the complex numbers, uses the resultant formula for the inverse of an automorphism (McKay and Wang) and a differential equation associated with the fact that the Jacobian of the automorphism is a nonzero constant. Then the required divisibility condition on the degrees of the images of x and y follows from the fact that this differential equation must have a rational function solution.

1. Introduction

In 1942 Jung [6] first proved that every automorphism of the polynomial ring in two variables over a field of characteristic 0 is a composition of elementary automorphisms (see Section 4). In 1953 Van der Kulk [13] extended Jung's theorem to a field of arbitrary characteristic. Since then several proofs have appeared: Gutwirth [5] in 1961, Shafarevich [12] in 1966, Rentschler [11] in 1968, Makar-Limanov [8] in 1970, Nagata [10] in 1972, Abhyankar and Moh [1] in 1975, Dicks [3] in 1983. The techniques used are different. Gutwirth (Evyatar) studied numerical properties of pencils of curves with a common multiple base point satisfying a number of conditions relative to the infinitely near points to this base point. Shafarevich used the fact that every birational isomorphism of projective surfaces is a product of dilatations. Using Dixmier's work [4] on automorphisms of the first Weyl algebra, Rentschler proved that any locally nilpotent derivation of $k[x, y]$ (where k is a field of characteristic 0) is conjugate by a composition of certain elementary automorphisms to a derivation of the form $f(y)(\partial/\partial x)$ (where $f(y)$ is a polynomial in y), from which the automorphism theorem follows.

0022-4049/88/\$3.50

Makar-Limanov considered different linear orderings on the free abelian group with two generators, to obtain information about leading forms. Nagata gave two proofs, one geometric [10, §1.2, pp. 21–28], one numerical [10, §1.3, pp. 28–32]. Abhyankar and Moh used Newton–Puiseux expansion, characteristic pairs and approximate roots to prove [1, (4.2) Main Theorem, p. 161] first and then deduced [1, (1.5) Automorphism theorem, p. 151]. Dicks gave a modified version of Makar-Limanov's proof. Based on the automorphism theorem, one can derive a more precise statement: the automorphism group of $k[x, y]$, where k is a field, is the fibre coproduct of its affine subgroup $A(2)$ and de Jonquières (i.e., triangular) subgroup $J(2)$ over their intersection $C(2) = A(2) \cap J(2)$; in other words, the automorphism group is the free product of $A(2)$ and $J(2)$ amalgamated along $C(2)$. The last statement was derived in [10, Theorem 3.3, p. 31; 7, Theorem 2, p. 454; 13, Theorem 4, p. 245; 2, the last theorem on p. 111; 3, Theorem 3, p. 160], and stated in [12, Theorem 7, p. 211]. (Note that the 'fact' stated in [12, second paragraph on p. 209], now known as the Jacobian conjecture, has not been proved yet.)

We present an elementary proof in this paper, which is self-contained except for the inversion formula and a simple derivation about resultants [9, Theorem 12, p. 252, and Theorem 5, p. 249]. This information is explicitly recorded in the beginning of Section 4. Besides being an elementary and different approach, it is presented for another reason. It suggests that information about automorphisms of $\mathbb{C}[x, y, z]$ can be determined by finding the inversion formula for $\mathbb{C}[x, y, z]$. As Nagata states "... in order to investigate the three variable case or more general cases, it is worthy to know many different proofs of the two variable case."[10, Preface].

2. Fundamental differential equation

Throughout we use the following notations. $\mathbb{C}$ denotes the field of complex numbers, $\mathbb{C}[U]$ a polynomial ring over $\mathbb{C}$, $\mathbb{C}(U)$ a rational function field over $\mathbb{C}$, and $\mathscr{L} = \mathbb{C}(U)((V^{-1}))$ the field of formal Laurent series in V^{-1} with coefficients in $\mathbb{C}(U)$.

$$A(U, V) = \alpha(U)V^a + \alpha_{a-1}(U)V^{a-1} + \cdots,$$
$$B(U, V) = \beta(U)V^b + \beta_{b-1}(U)V^{b-1} + \cdots$$

are nonzero Laurent series in $\mathscr{L}$, where $\alpha(U) \neq 0$ and $\beta(U) \neq 0$. Note that the powers of V are decreasing. $\alpha(V)V^a$ is called the *leading term* of A, $\alpha(U)$ the *leading coefficient* of A, and a the *V-degree* of A. We also define $\deg_V 0 = -\infty$. We shall assume that the Jacobian of A and B with respect to U and V is nonzero and its V-degree is $c - 1$ so that

$$\frac{\partial(A, B)}{\partial(U, V)} = \gamma(U)V^{c-1} + \gamma_{c-2}(U)V^{c-2} + \cdots$$

for some $\gamma(U) \neq 0$.

If a Laurent series $D(U, V)$ in $\mathscr{L}$ has leading term 1, say

$$D(U, V) = 1 + \beta_{-1}(U)V^{-1} + \beta_{-2}(U)V^{-2} + \cdots,$$

and r is a rational number, then D admits unique powers D^r with leading term 1; namely, we can apply the binomial expansion to

$$\{1 + [\beta_{-1}(U)V^{-1} + \beta_{-2}(U)V^{-2} + \cdots]\}^r.$$

Note that

$$A(U, V) = \alpha(U)V^a A_{[1]}(U, V)$$

where $A_{[1]}(U, V)$ has leading term 1. As a result, an rth power of $A(U, V)$ exists in $\mathscr{L}$ if and only if an rth power of its leading term exists in $\mathscr{L}$. Note that $\mathbb{C}[U, V]$ embeds into $\mathscr{L}$ by arranging any polynomial in U and V in decreasing powers of V. Thus, since $\mathscr{L}$ is a field, $\mathbb{C}(U, V)$ embeds into $\mathscr{L}$. By working in $\mathscr{L}$ instead of $\mathbb{C}(U, V)$ we have the advantage of knowing that (an) $[A(U, V)]^r$ exists in $\mathscr{L}$ whenever (an) $[\alpha(U)V^a]^r$ exists in $\mathscr{L}$.

Lemma 1. *Let A, B, $a = \deg_V A$, $b = \deg_V B$ be as above. If*

$$c - 1\left(= \deg_V \frac{\partial(A, B)}{\partial(U, V)}\right) < a + b - 1$$

and $a \neq 0$, then a (b/a)th power of A exists in $\mathscr{L} = \mathbb{C}(U)((V^{-1}))$ and

$$\deg_V(B - \lambda A^{b/a}) < \deg_V B$$

for some nonzero λ in $\mathbb{C}$.

Proof. Under the hypothesis on degrees,

$$\begin{vmatrix} \alpha'(U)V^a & \alpha(U)aV^{a-1} \\ \beta'(U)V^b & \beta(U)bV^{b-1} \end{vmatrix} = 0.$$

Hence $[\beta(U)^a\alpha(U)^{-b}]' = 0$ and so $\beta(U)^a = \lambda^a\alpha(U)^b$ for some nonzero λ in $\mathbb{C}$. Thus, putting

$$C(U, V) = \lambda^{-1}\beta(U)V^b[A_{[1]}(U, V)]^{b/a},$$

we have

$$C(U,V)^a = \lambda^{-a}\beta(U)^a V^{ab} A_{[1]}(U,V)^b = \alpha(U)^b V^{ab} A_{[1]}(U,V)^b$$
$$= A(U,V)^b$$

so C is a (b/a)th power of A; we shall write $C = A^{b/a}$. Since $\lambda[A(U,V)]^{b/a} = \lambda C(U,V) = \beta(U)V^b[A_{[1]}(U,V)]^{b/a}$ has the same leading term as $B(U,V)$, $\deg_V(B - \lambda A^{b/a}) < \deg_V B$. $\square$

Theorem 2 (Fundamental Differential Equation). *Let*

$$A(U,V) = \alpha(U)V^a + \cdots, \qquad B(U,V) = \beta(U)V^b + \cdots,$$
$$\frac{\partial(A,B)}{\partial(U,V)} = \gamma(U)V^{c-1} + \cdots$$

be as above. If $a \neq 0$, then there exists a $\delta(U)$ in $\mathbb{C}(U)$ such that

$$\frac{\gamma(U)}{\delta(U)} = c\,\frac{\alpha'(U)}{\alpha(U)} - a\,\frac{\delta'(U)}{\delta(U)}$$

or equivalently

$$\frac{\gamma(U)}{\delta(U)} = \frac{[\alpha(U)^c\delta(U)^{-a}]'}{\alpha(U)^c\delta(U)^{-a}}\ .$$

Proof. In general, $\deg_V(\partial(A,B)/\partial(U,V)) \leq \deg_V A + \deg_V B - 1$ or equivalently, $c \leq a + b$.

Case 1. $c = a + b$.

$$\frac{\partial(A,B)}{\partial(U,V)} = \begin{vmatrix} \alpha'(U)V^a & \alpha(U)aV^{a-1} \\ \beta'(U)V^b & \beta(U)bV^{b-1} \end{vmatrix} + \text{terms of lower } V\text{-degree}$$
$$= [b\alpha'(U)\beta(U) - a\alpha(U)\beta'(U)]V^{a+b-1} + \text{terms of lower } V\text{-degree}\,.$$

On the other hand, $\partial(A,B)/\partial(U,V) = \gamma(U)V^{c-1} +$ terms of lower V-degree, with $\gamma(U) \neq 0$. Thus

$$\gamma(U) = b\alpha'(U)\beta(U) - a\alpha(U)\beta'(U)\,,$$
$$\frac{\gamma(U)}{\alpha(U)\beta(U)} = b\,\frac{\alpha'(U)}{\alpha(U)} - a\,\frac{\beta'(U)}{\beta(U)} = c\,\frac{\alpha'(U)}{\alpha(U)} - a\,\frac{[\alpha(U)\beta(U)]'}{\alpha(U)\beta(U)}\ .$$

Setting $\delta(U) = \alpha(U)\beta(U)$, we have the desired result.

Case 2. $c < a + b$.

We *claim* that there exists a $B_s = B - \mathbb{C}$-linear combination of rational powers of A such that

$$\deg_V B_s = c - a\,.$$

Note then that

$$\frac{\partial(A, B_s)}{\partial(U, V)} = \frac{\partial(A, B)}{\partial(U, V)}$$

has V-degree $c - 1$ and $c = a + (c - a) = \deg_V A + \deg_V B_s$, whence (A, B_s) is as in Case 1. Hence the theorem follows, from Case 1, with

$$\delta(U) = \alpha(U) \times \text{leading coefficient of } B_s\,.$$

We establish the claim as follows. By Lemma 1, we can adjust B, by subtracting $\lambda_1 A^{r_1}$ to obtain

$$B_1 = B - \lambda_1 A^{r_1}$$

with $\deg_V B_1 \leq \deg_V B - 1$ without changing the Jacobian. As before, $c \leq a + \deg_V B_1$ or equivalently $\deg_V B_1 \geq c - a$. If there is strict inequality, then the process can be repeated to obtain

$$B_2 = B_1 - \lambda_2 A^{r_2} = B - \lambda_1 A^{r_1} - \lambda_2 A^{r_2}$$

with $\deg_V B_2 \leq \deg_V B_1 - 1$ without changing the Jacobian. Since $c - a$ is a lower bound for the V-degrees of $B, B_1, B_2, \ldots$, the process must stop. Therefore there is a B_s in $\mathscr{L}$ such that

(i) B_s is obtained from B by subtracting a finite $\mathbb{C}$-linear combination of rational powers of A;

(ii) $\deg_V B_s = c - a$. □

Corollary 3. *If $b \neq 0$, then there exists an $\varepsilon(U)$ in $\mathbb{C}(U)$ such that*

$$\frac{\gamma(U)}{\varepsilon(U)} = c\,\frac{\beta'(U)}{\beta(U)} - b\,\frac{\varepsilon'(U)}{\varepsilon(U)}\,. \qquad \square$$

3. A lemma on logarithmic derivatives

In the next section we will note that the Jacobian condition applied to two polynomials in $\mathbb{C}[x, y]$ suggests that we are interested in the fundamental differential equation for the case of $\partial(A, B)/\partial(U, V)$ with a special type of leading V-terms. To study this differential equation, our method is to embed $\mathbb{C}(U)$ into $\mathbb{C}((U-\Theta))$, the field of formal Laurent series in $U-\Theta$, for various $\Theta \in \mathbb{C}$, and then compare the degrees and orders of both sides of the differential equation.

For any rational function $\mu(U)/\nu(U)$, with $\mu(U), \nu(U) \in \mathbb{C}[U]$, define $\deg(\mu/\nu) = \deg \mu - \deg \nu$. Then $-\deg$ is a discrete valuation on $\mathbb{C}(U)$. This discrete valuation will also be denoted by v_∞. To define $v_\Theta(\mu/\nu)$ for $\Theta \in \mathbb{C}$, expand μ/ν as a Laurent series in powers of $U-\Theta$. Then $v_\Theta(\mu/\nu)$ is the smallest integer i such that $(U-\Theta)^i$ appears with a nonzero coefficient in this expansion. The mapping v_Θ is a discrete valuation on $\mathbb{C}((U-\Theta))$. In short,

$$\nu_\infty\left(\frac{\mu}{\nu}\right) = -\deg \mu + \deg \nu = \text{order of } \frac{\mu}{\nu} \text{ as a Laurent series in } U^{-1},$$

$$v_\Theta\left(\frac{\mu}{\nu}\right) = \text{order of } \frac{\mu}{\nu} \text{ as a Laurent series in } U-\Theta .$$

In terms of the unique factorization on $\mathbb{C}(U)$, the discrete valuations v_∞, v_Θ on $\mathbb{C}(U)$ can be expressed as follows: Let

$$\psi(U) = \lambda \prod_{\omega \in \mathbb{C}} (U-\omega)^{e_\omega}$$

be the unique factorization of a nonzero element $\psi(U)$ of $\mathbb{C}(U)$ where some of the integers e_ω may be negative, and $\lambda \neq 0$ in $\mathbb{C}$. Then

$$v_\infty(\psi) = -\sum_{\omega \in \mathbb{C}} e_\omega , \qquad v_\Theta(\psi) = e_\Theta .$$

Hence we also have the summation formula

$$\sum_{p \in \mathbb{C} \cup \{\infty\}} v_p = 0 .$$

In our situation, as we shall see in Section 4, the most crucial information is obtained from $v_\infty + v_0$.

The next lemma provides useful information about these valuations applied to a logarithmic derivative.

Lemma 4. *Let $\psi(U)$ be a nonzero rational function in U with coefficients in $\mathbb{C}$, and let Θ be in $\mathbb{C}$.*

(i) $$v_\Theta\left(\frac{\psi'}{\psi}\right) \text{ is } \begin{cases} -1 & \Leftrightarrow \quad v_\Theta(\psi) \neq 0 , \\ >-1 & \Leftrightarrow \quad v_\Theta(\psi) = 0 . \end{cases}$$

(ii) $$v_\infty\left(\frac{\psi'}{\psi}\right) \text{ is } \begin{cases} 1 & \Leftrightarrow \quad v_\infty(\psi) \neq 0 , \\ >1 & \Leftrightarrow \quad v_\infty(\psi) = 0 . \end{cases}$$

Or equivalently,

$$\deg\left(\frac{\psi'}{\psi}\right) \text{ is } \begin{cases} -1 & \Leftrightarrow \quad \deg \psi \neq 0\,, \\ <-1 & \Leftrightarrow \quad \deg \psi = 0\,. \end{cases}$$

Proof. Let

$$\psi(U) = \lambda \prod_{\omega \in \mathbb{C}} (U - \omega)^{v_\omega(\psi)}$$

be the unique factorization of $\psi(U)$, where $\lambda \neq 0$ is in $\mathbb{C}$. Then

$$\frac{\psi'(U)}{\psi(U)} = \sum_{\omega \in \mathbb{C}} \frac{v_\omega(\psi)}{U - \omega}\,.$$

For $v_\omega(\psi) \neq 0$,

$$v_\Theta\left(\frac{v_\omega(\psi)}{U - \omega}\right) = \begin{cases} -1 & \text{if } \Theta = \omega\,, \\ 0 & \text{if } \Theta \neq \omega\,. \end{cases}$$

The discrete valuation of a sum is greater than or equal to the minimum of the discrete valuation of the individual terms, and when the minimum occurs only at one term, then the discrete valuation is the minimum. This proves part (i).

(ii) Write $\psi(U) = \mu(U)/\nu(U)$ with $\mu(U)$, $\nu(U)$ in $\mathbb{C}[U]$ and $\neq 0$. Then $\psi'/\psi = (\mu'/\mu) - (\nu'/\nu)$ and $\deg(\psi'/\psi) = \deg(\mu'\nu - \mu\nu') - \deg \mu - \deg \nu$. Because $\deg \mu'\nu = \deg \mu\nu' = \deg \mu + \deg \nu - 1$, $\deg(\psi'/\psi)$ is either <-1 or -1 depending upon whether or not the highest power terms in $\mu'\nu$ and $\mu\nu'$ are identical. This happens if and only if $\deg \mu = \deg \nu$, i.e., if and only if $\deg \psi = 0$. □

Remark. Part (ii) of Lemma 4 can also be derived from part (i) by noting that

$$v_\infty(\psi'(U)) = v_\infty\left(\frac{\mathrm{d}\psi}{\mathrm{d}U}\right) = v_\infty\left(\frac{\mathrm{d}\psi}{\mathrm{d}U^{-1}}\right) + v_\infty\left(\frac{\mathrm{d}U^{-1}}{\mathrm{d}U}\right) = v_\infty\left(\frac{\mathrm{d}\psi}{\mathrm{d}U^{-1}}\right) - 2\,.$$

The gist of Lemma 4 is that for each $\Theta \in \mathbb{C}$, either $v_\Theta(\psi'/\psi) = -1$ or $v_\Theta(\psi) = 0$; either $v_\infty(\psi'/\psi) = 1$ or $v_\infty(\psi) = 0$.

4. Automorphisms of $\mathbb{C}[x, y]$

If

$$\phi : \mathbb{C}[x, y] \to \mathbb{C}[x, y]\,, \qquad x \mapsto f(x, y)\,, \qquad y \mapsto g(x, y)\,,$$

defines an automorphism of $\mathbb{C}[x, y]$ and $n = \deg f(0, t) \geq 1$, $m = \deg g(0, t) \geq 1$, we want to show that $n \mid m$ or $m \mid n$.

This argument is self-contained except for one fact from [9, Theorem 12, p. 252, and Theorem 5, p. 249], which we now state. If $\phi^{-1}(x) = F(x, y)$, then

$$F(x, y) = \sum_{rn+sm\leq mn} F_{r,s}x^r y^s$$

where $F_{r,s} \in \mathbb{C}$, and

$$\sum_{rn+sm=mn} F_{r,s}x^r y^s = \mu(x^{\tilde{m}} - \rho y^{\tilde{n}})^d$$

where $d = \text{g.c.d.}(m, n)$, $\tilde{m} = m/d$, $\tilde{n} = n/d$ and μ, ρ are nonzero elements of $\mathbb{C}$. In other words, if a monomial $x^r y^s$ appears in $F(x, y)$ with a nonzero coefficient, then (r, s) is within the triangle whose vertices are $(m, 0)$, $(0, n)$, $(0, 0)$, see Fig. 1, and moreover, the sum of terms along the hypotenuse is $\mu(x^{\tilde{m}} - \rho y^{\tilde{n}})^d$.

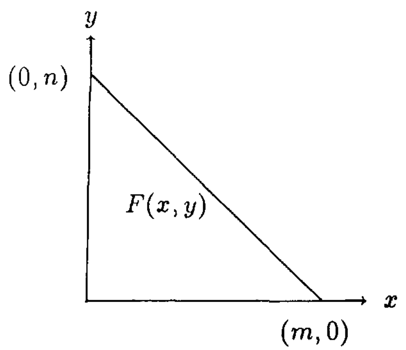

Fig. 1.

To pick up terms along the hypotenuse, we shall assign

$$\text{weight}(x) = \tilde{n}\ , \qquad \text{weight}(y) = \tilde{m}\ .$$

Then the terms on the hypotenuse are those whose weights are $\tilde{m}n = m\tilde{n} = \tilde{m}\tilde{n}d$.

To relate the above information to the previous sections, we fix the following notation. Pick a pair of positive integers u, v such that $u\tilde{m} - v\tilde{n} = 1$. As

$$\begin{bmatrix} u & \tilde{n} \\ v & \tilde{m} \end{bmatrix}^{-1} = \begin{bmatrix} \tilde{m} & -\tilde{n} \\ -v & u \end{bmatrix},$$

we can embed $\mathbb{C}(x, y)$ onto $\mathbb{C}(U, V)$ by

$$x = U^u V^{\tilde{n}}\ , \qquad y = U^v V^{\tilde{m}}\ .$$

Then, with $\text{weight}(x) = \tilde{n}$, $\text{weight}(y) = \tilde{m}$, the weight of any monomial in x, y is exactly the exponent of V after the change of variables. With $F(x, y) = \phi^{-1}(x)$

and $G(x, y) = \phi^{-1}(y)$, set

$$A(U, V) = F(U^u V^{\tilde{n}}, U^v V^{\tilde{m}})$$

and

$$B(U, V) = G(U^u V^{\tilde{n}}, U^v V^{\tilde{m}}) .$$

Clearly $A(U, V)$ and $B(U, V)$ are nonzero elements of $\mathscr{L} = \mathbb{C}(U)((V^{-1}))$. Since

$$\begin{aligned} A(U, V) &= \sum_{r\tilde{n} + s\tilde{m} \leq \tilde{m}\tilde{n}d} F_{r,s} U^{ru+sv} V^{r\tilde{n}+s\tilde{m}} \\ &= \alpha(U)V^a + (\text{terms of } V\text{-degree} < a) , \end{aligned}$$

the leading term $\alpha(U)V^a$ of $A(U, V)$ is

$$\begin{aligned} \sum_{r\tilde{n} + s\tilde{m} = \tilde{m}\tilde{n}d} F_{r,s} U^{ru+sv} V^{\tilde{m}\tilde{n}d} &= \mu[(U^u V^{\tilde{n}})^{\tilde{m}} - \rho(U^v V^{\tilde{m}})^{\tilde{n}}]^d \\ &= \mu U^{v\tilde{n}d}[U^{u\tilde{m}-v\tilde{n}} - \rho]^d V^{\tilde{m}\tilde{n}d} = \mu U^{nv}[U - \rho]^d V^{\tilde{m}\tilde{n}d} . \end{aligned}$$

Note that there are $d + 1$ lattice points on the hypotenuse.

By the chain rule, the product of $\partial(F, G)/\partial(x, y)$ and $\partial(f, g)/\partial(x, y)$ equals 1 and so $\partial(F, G)/\partial(x, y)$ is a nonzero element of $\mathbb{C}$ which we may assume to be 1. Then

$$\begin{aligned} \frac{\partial(A, B)}{\partial(U, V)} &= \frac{\partial(F, G)}{\partial(x, y)} \cdot \frac{\partial(x, y)}{\partial(U, V)} = 1 \begin{vmatrix} u & \tilde{n} \\ v & \tilde{m} \end{vmatrix} U^{u+v-1} V^{\tilde{n}+\tilde{m}-1} \\ &= U^{u+v-1} V^{\tilde{n}+\tilde{m}-1} . \end{aligned}$$

Thus the leading term $\gamma(U)V^{c-1}$ of $\partial(A, B)/\partial(U, V)$ as a Laurent series in V^{-1} is given by

$$\gamma(U) = U^{u+v-1} , \qquad c = \tilde{n} + \tilde{m} .$$

Recall from above that the leading term $\alpha(U)V^a$ of $A(U, V)$ is given by

$$\alpha(U) = \mu U^{nv}[U - \rho]^d , \qquad a = \tilde{m}\tilde{n}d .$$

According to Theorem 2, there is a $\delta(U)$ in $\mathbb{C}(U)$ such that

$$(*) \qquad \frac{U^{u+v-1}}{\delta(U)} = \frac{\psi'(U)}{\psi(U)} ,$$

with

$$\begin{aligned} \psi(U) = \alpha(U)^c \delta(U)^{-a} &= \mu^{\tilde{n}+\tilde{m}} U^{nv(\tilde{n}+\tilde{m})}[U - \rho]^{d(\tilde{n}+\tilde{m})} \delta(U)^{-\tilde{m}\tilde{n}d} \\ &= \mu^{\tilde{n}+\tilde{m}} U^{\tilde{n}v(n+m)}[U - \rho]^{n+m} \delta(U)^{-\tilde{m}\tilde{n}d} . \end{aligned}$$

Applying Lemma 4 to Equation (*) with $\Theta = 0$, we have

$$(u+v-1) - v_0(\delta)$$
$$\text{is} \begin{cases} -1 & \Leftrightarrow \quad \tilde{n}v(n+m) - \tilde{m}\tilde{n}dv_0(\delta) \neq 0\,, \\ >-1 & \Leftrightarrow \quad \tilde{n}v(n+m) - \tilde{m}\tilde{n}dv_0(\delta) = 0\,. \end{cases}$$

$$(u+v-1) - \deg(\delta)$$
$$\text{is} \begin{cases} -1 & \Leftrightarrow \quad \tilde{n}v(n+m) + (n+m) - \tilde{m}\tilde{n}d\deg(\delta) \neq 0\,, \\ <-1 & \Leftrightarrow \quad \tilde{n}v(n+m) + (n+m) - \tilde{m}\tilde{n}d\deg(\delta) = 0\,. \end{cases}$$

In other words, there are two options for $v_0(\delta)$, and two options for $\deg(\delta)$:

$$v_0(\delta) = \begin{cases} u+v, \\ \dfrac{v(n+m)}{m} = u+v-\dfrac{1}{\tilde{m}}\,; \end{cases}$$

$$\deg(\delta) = \begin{cases} u+v\,, \\ \dfrac{v(n+m)}{m} + \dfrac{n+m}{\tilde{m}\tilde{n}d} = u+v+\dfrac{1}{\tilde{n}}\,. \end{cases}$$

Thus we have four options:

$$-v_\infty(\delta) - v_0(\delta) = \begin{cases} 0\,, \\ \dfrac{1}{\tilde{n}}\,, \\ \dfrac{1}{\tilde{m}}\,, \\ \dfrac{1}{\tilde{n}} + \dfrac{1}{\tilde{m}}\,. \end{cases}$$

The fourth option implies $\tilde{n} = \tilde{m} = 1$ since the left-hand side is an integer, and $\tilde{n}$, $\tilde{m}$ are relatively prime integers. The middle two options imply either $\tilde{n} = 1$ or $\tilde{m} = 1$. To dispose of the first option, we apply Lemma 4 to Equation (*) with $\Theta = \rho$ to show $-v_\infty(\delta) - v_0(\delta) > 0$. By applying Lemma 4, we have

$$-v_\rho(\delta)\ \text{is} \begin{cases} -1 & \Leftrightarrow \quad (n+m) - \tilde{m}\tilde{n}dv_\rho(\delta) \neq 0\,, \\ >-1 & \Leftrightarrow \quad (n+m) - \tilde{m}\tilde{n}dv_\rho(\delta) = 0\,. \end{cases}$$

Equivalently, $v_\rho(\delta) = 1$ or

$$0 < \frac{1}{\tilde{m}} + \frac{1}{\tilde{n}} = \frac{n+m}{\tilde{m}\tilde{n}d} = v_\rho(\delta) < 1\,.$$

Since $v_\rho(\delta)$ is an integer, $v_\rho(\delta)=1$. Similarly, for $\Theta \not\in \{0, \rho\}$, $v_\Theta(\delta)=1$ or 0. Thus

$$\delta(U)=\lambda U^e(U-\rho)\prod_{\Theta\neq 0,\rho}(U-\Theta)^{e_\Theta}$$

where e is an integer, e_Θ is either 1 or 0, and λ is a nonzero element of $\mathbb{C}$. It follows that $-v_\infty(\delta)-v_0(\delta)=1+\sum_\Theta e_\Theta>0$. Consequently, we have

Lemma 5 (Automorphism Lemma). *If ϕ is a $\mathbb{C}$-algebra automorphism of $\mathbb{C}[x, y]$ with $\phi(x)=f(x, y)$, $\phi(y)=g(x, y)$, $\deg f(0, t)=n\geq 1$, $\deg g(0, t)=m\geq 1$, then $n\mid m$ or $m\mid n$.* □

An automorphism ϕ of $\mathbb{C}[x, y]$ is *tame* if ϕ is a finite (compositional) product of automorphisms of the following elementary types:

(i) $\quad x\mapsto \lambda_{11}x+\lambda_{12}y+\lambda_{13}\,,\qquad y\mapsto\lambda_{21}x+\lambda_{22}y+\lambda_{23}$

with

$$\begin{vmatrix}\lambda_{11} & \lambda_{12}\\ \lambda_{21} & \lambda_{22}\end{vmatrix}\neq 0 \quad\text{and}\quad \lambda_{ij}\in\mathbb{C}\,;$$

(ii) $\quad x\mapsto x\,,\qquad y\mapsto y+h(x)$

with $h(x)\in\mathbb{C}[x]$.

Theorem 6 (Automorphism Theorem). *Every $\mathbb{C}$-algebra automorphism of $\mathbb{C}[x, y]$ is tame.*

Proof. Let ϕ be an automorphism of $\mathbb{C}[x, y]$ with $\phi(x)=f(x, y)$, $\phi(y)=g(x, y)$ and $n=\deg f(0, t)$, $m=\deg f(0, t)$.

If $n=0$, then $f(x, y)$ is a polynomial in $\mathbb{C}[x]$ and

$$\frac{\partial(f, g)}{\partial(x, y)}=\frac{\mathrm{d}f}{\mathrm{d}x}\cdot\frac{\partial g}{\partial y}$$

is a nonzero element of $\mathbb{C}$. Hence f is a linear polynomial in $\mathbb{C}[x]$, and g is the sum of a linear polynomial in $\mathbb{C}[y]$ and a polynomial in $\mathbb{C}[x]$. Therefore ϕ is tame in this case. Similarly ϕ is tame if $m=0$.

Now consider $n\geq 1$ and $m\geq 1$. Then

$$f(x, y)=f_n y^n+f_{n-1}(x)y^{n-1}+\cdots+f_0(x)\,,$$
$$g(x, y)=g_m y^m+g_{m-1}(x)y^{m-1}+\cdots+g_0(x)$$

where $f_i(x)$, $g_j(x)\in\mathbb{C}[x]$, and, by the observation at the beginning of this section, f_n and g_m are nonzero elements of $\mathbb{C}$. By Lemma 5, either $n\mid m$ or $m\mid n$. If $n\mid m$, let $e = m/n$ and $\lambda = g_m/f_n^e$, then

$$\deg_y(g - \lambda f^e) < \deg_y g = m .$$

The replacement of g by $g - \lambda f^e$ is a tame automorphism. By induction on the maximum of $\deg_y \phi(x)$ and $\deg_y \phi(y)$, it follows that ϕ is tame. □

Acknowledgment

We would like to thank Hyman Bass for reading through the manuscript and making helpful suggestions.

References

[1] S.S. Abhyankar and T.T. Moh, Embeddings of the line in the plane, J. Reine Angew. Math. 276 (1975) 148–166.
[2] R.C. Alperin, Homology of the group of automorphisms of $k[x, y]$, J. Pure Appl. Algebra 15 (1979) 109–115.
[3] W. Dicks, Automorphisms of the polynomial ring in two variables, Publ. Sec. Mat. Univ. Autònoma Barcelona 27 (1983) 155–162.
[4] J. Dixmier, Sur les algèbres de Weyl, Bull. Soc. Math. France 96 (1968) 209–242.
[5] A. Gutwirth, An inequality for certain pencils of plane curves, Proc. Amer. Math. Soc. 12 (1961) 631–638.
[6] H.W.E. Jung, Über ganze birationale Transformationen der Ebene, J. Reine Angew. Math. 184 (1942) 161–174.
[7] T. Kambayashi, On the absence of nontrivial separable forms of the affine plane, J. Algebra 35 (1975) 449–456.
[8] L.G. Makar-Limanov, On automorphisms of certain algebras, Candidate's Dissertation, Moscow State University, 1970. (In Russian.)
[9] J.H. McKay and S.S.-S. Wang, An inversion formula for two polynomials in two variables, J. Pure Appl. Algebra 40 (1986) 245–257.
[10] M. Nagata, On automorphism group of $k[x, y]$, Lectures in Mathematics 5 (Kinokuniya Book Store, Tokyo, 1972).
[11] R. Rentschler, Opérations du groupe additif sur le plan affine, C.R. Acad. Sci. Paris Sér. A 267 (1968) 384–387.
[12] I.R. Shafarevich, On some infinite dimensional groups, Rend. Mat. Appl. 25 (1966) 208–212.
[13] W. Van der Kulk, On polynomial rings in two variables, Nieuw Arch. Wisk. (3) 1 (1953) 33–41.
[14] D. Wright, The amalgamated free product structure of $GL_2(k[x_1, \ldots, x_n])$ and the weak Jacobian theorem for two variables, J. Pure Appl. Algebra 12 (1978) 235–251.